

H.R. 3635 will reduce our dependence on foreign sources of supplies like PPE by boosting domestic manufacturing to make these products here in the United States. It would also make critical improvements to our Strategic National Stockpile to ensure it is full and items are ready to be deployed when needed.

Strengthening our stockpile of PPE and domestic manufacturing has never been more important for our economy and our national security. I urge my colleagues to support this legislation so we can be better prepared for the next public health emergency.

Madam Speaker, additionally, I am proud to have introduced H.R. 4032, the Open RAN Outreach Act, a bill that will also be considered by this House today.

The Open RAN Outreach Act will strengthen our telecommunications supply chains and help protect small and rural communications providers from Chinese-backed companies. Protecting our supply chains and pushing back against China are more critical than ever before, especially for our vulnerable telecommunications networks. Providers backed by the Chinese Communist Party have tried to undercut the market and expand their outreach, particularly in our underserved rural communities.

By passing H.R. 4032, we can encourage a competitive market of trusted vendors to expand network access across our country. Just like H.R. 3635, this bill is also critical not just for our economy, but for our national security.

Madam Speaker, I urge my colleagues to support it as well.

Mr. PALLONE. Madam Speaker, I reserve the balance of my time.

Mr. GUTHRIE. Madam Speaker, I yield 3 minutes to the gentlewoman from Indiana (Mrs. WALORSKI), a member of the Committee on Ways and Means.

Mrs. WALORSKI. Madam Speaker, I rise today in support of H.R. 3635, the Strengthening America's Strategic National Stockpile Act. A key lesson from the pandemic has been the absolute need to end our dependence on the Chinese Communist Party for the production of medicines, personal protective equipment, and other critical medical supplies.

Now more than ever, we know that secure and resilient supply chains are vital to the safety and success of the American people. It is so critical to focus on breaking our dependency on China and move domestic manufacturing of PPE products back home to the U.S.

Early on in the pandemic, the Department of Homeland Security concluded that China "intentionally concealed the severity" of this virus so they could hoard PPE by blocking exports and buying it up through its state-owned enterprises, a theory that has been confirmed time and time again.

In March of 2020, the New York Times reported that factories in China

were not authorized to export masks, and all the while bought up much of the world's supply first. In February of last year, Chinese entrepreneurs and aid groups visited pharmacies in affluent countries and emerging markets, buying masks in bulk to send to China.

Similarly, the Sydney Morning Herald reported that the Greenland Group, a Chinese government-backed property giant, instructed its employees worldwide—even accountants and receptionists and their HR teams—to stop what they were doing and bulk buy as many medical supplies as they could in January and February of 2020.

It is quite simple. We must not trust the Chinese Communist Party. The bipartisan legislation before us today is a strong step in the right direction toward strengthening American manufacturing of PPE in Indiana and across the rest of the country.

Specifically, it includes the Medical Supplies for Pandemics Act I led with Congresswoman DINGELL, that would enhance medical supply chain elasticity, improve the domestic production of PPE, and partner with private industry to refresh and replenish existing stocks of medical supplies.

Our legislation takes other important measures, such as supporting State efforts to expand and maintain our own stockpiles, improving maintenance of the national stockpile to ensure it is in good working order and allow the transfer of stockpile items nearing their expiration dates to other federal agencies.

To prepare for the next crisis and better protect frontline healthcare workers, we need to boost U.S. manufacturing of PPE and strengthen the Strategic National Stockpile.

Madam Speaker, I urge support, and I thank my colleagues.

Mr. GUTHRIE. Madam Speaker, I am prepared to close, and I yield myself such time as I may consume.

Madam Speaker, I urge support of this piece of legislation.

Fortunately, the last big pandemic that came across the country was in 1918, the flu pandemic, so over 100 years. What we learned, although it was well-planned and all, the Strategic National Stockpile, until you really face a pandemic like we have, you don't truly understand exactly everything you need to do, although the Strategic National Stockpile was there, it was drawn from, it was used. There were a lot of lessons learned.

Madam Speaker, it is important that we apply these lessons. I appreciate my colleagues for doing this, moving forward. Hopefully, it will be another 100 years or more before we have to use the Strategic National Stockpile, but it certainly is prudent that we are ready.

Madam Speaker, I urge the passage of this legislation, and I yield back the balance of my time.

Mr. PALLONE. Madam Speaker, I agree with my colleague that what this bill does is basically take the lessons that we learned from the pandemic

about what can be done to improve the Strategic National Stockpile for the future.

Madam Speaker, I ask everyone to support the bill on a bipartisan basis, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. PALLONE) that the House suspend the rules and pass the bill, H.R. 3635.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. GOOD of Virginia. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

SECURE EQUIPMENT ACT OF 2021

Mr. PALLONE. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 3919) to ensure that the Federal Communications Commission does not approve radio frequency devices that pose a national security risk, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3919

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure Equipment Act of 2021".

SEC. 2. UPDATES TO EQUIPMENT AUTHORIZATION PROCESS OF FEDERAL COMMUNICATIONS COMMISSION.

(a) RULEMAKING.—

(1) *IN GENERAL.*—Not later than 1 year after the date of the enactment of this Act, the Commission shall adopt rules in the proceeding initiated in the Notice of Proposed Rulemaking in the matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program (ET Docket No. 21–232; FCC 21–73; adopted June 17, 2021), in accordance with paragraph (2), to update the equipment authorization procedures of the Commission.

(2) *UPDATES REQUIRED.*—In the rules adopted under paragraph (1), the Commission shall clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(a)).

(3) APPLICABILITY.—

(A) *IN GENERAL.*—In the rules adopted under paragraph (1), the Commission may not provide for review or revocation of any equipment authorization granted before the date on which such rules are adopted on the basis of the equipment being on the list described in paragraph (2).

(B) *RULE OF CONSTRUCTION.*—Nothing in this section may be construed to prohibit the Commission, other than in the rules adopted under paragraph (1), from—

(i) *examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the list described in paragraph (2); or*

(ii) adopting rules providing for any such review or revocation.

(b) DEFINITION.—In this section, the term “Commission” means the Federal Communications Commission.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Louisiana (Mr. SCALISE) each will control 20 minutes.

The Chair recognizes the gentleman from New Jersey.

□ 1645

GENERAL LEAVE

Mr. PALLONE. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 3919.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from New Jersey?

There was no objection.

Mr. PALLONE. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in support of H.R. 3919, the Secure Equipment Act of 2021.

Two years ago, we came together on a bipartisan basis to enact the Secure and Trusted Communications Act, legislation that I proudly authored. That bill was an important first step toward securing commercial communications networks in the United States from untrusted foreign adversaries. Among other things, it prohibits certain funds provided by the Federal Communications Commission from being used to purchase or obtain network equipment and services from certain untrusted vendors.

While that legislation established an important foundation and has made great strides in helping secure our communications networks, we have the opportunity today to take the next step by applying those same principles to the FCC’s equipment authorization process. We know our adversaries will use any and all potential avenues to weaken our networks, and therefore, we must remain vigilant and prevent it before they can do so.

H.R. 3919 simply requires the FCC to update its equipment authorization rules so that, going forward, the agency will no longer review or approve any application for equipment from vendors that have been determined to be a threat to our national security.

Importantly, while this bill focuses only on the applications that the agency is in the process of reviewing or will receive in the future, it does not prevent the FCC from later studying whether it should review equipment previously authorized but which is now known to pose a threat.

Over the past several years, the Energy and Commerce Committee has worked, on a bipartisan basis, on important security issues, and I commend Representatives Eshoo and Scalise for continuing in that tradition through

their leadership and bipartisan work on this legislation.

Madam Speaker, I urge my colleagues to support the Secure Equipment Act of 2021, and I reserve the balance of my time.

Mr. SCALISE. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I want to thank Chairman PALLONE and Ranking Member RODGERS of the full committee, as well as Ranking Member LATTA and Chairman DOYLE of the Communications and Technology Subcommittee, for helping bring my bill, H.R. 3919, the Secure Equipment Act, to the House floor.

Madam Speaker, I also want to especially thank Congresswoman ESHOO for partnering with me on this bill. We have worked on a number of telecommunications laws, and this is yet another example of Congresswoman ESHOO and I coming together, and our staffs, to address a very important threat to American families.

Madam Speaker, my bill is about one thing, and that is stopping the Chinese Communist Party and Chinese companies that act on their behalf from compromising our telecommunications networks and stopping them from jeopardizing American national security and the important data that all Americans hold sacred.

H.R. 3919, the Secure Equipment Act, puts a full stop to China infiltrating our networks by prohibiting the FCC from issuing equipment licenses to Chinese telecommunications equipment companies that are identified as national security threats.

This legislation builds off the important work of the Energy and Commerce Committee when it came together in a bipartisan manner in 2019, as Chairman PALLONE mentioned, on his critical legislation that will address the threat of China by getting the Secure and Trusted Communications Networks Act signed into law.

One of the requirements of that act instructed the FCC to publish a list of telecommunication equipment companies deemed to be national security threats. In fact, earlier this year, the FCC published that list of companies. As you can see, five companies ended up on that list. All of these companies are Chinese companies that are either partly or wholly owned by the Chinese Government and that have ties to the CCP.

Madam Speaker, we know all too well that the CCP wastes no time and no opportunity to expose American vulnerabilities and to try to undermine our national security. There are way too many examples of that.

Since all Chinese companies are subject to Chinese national security laws, at any point the CCP could choose to exploit these listed companies and require them to tap into their access in American networks to gain critical, sensitive data, both from individuals as well as sensitive government information.

While the 2019 law made great strides in thwarting the threat of China in our networks, U.S. carriers can still privately purchase equipment from these listed companies on the open market.

By prohibiting the FCC from issuing any equipment licenses to these companies that are listed as national security threats, our bill seeks to close the gap in existing law and slam the door on jeopardized Chinese equipment from threatening our American networks and from threatening the privacy and data of American families.

Madam Speaker, the time has never been more urgent. It is important that this body do all it can to stop the undue and malign influences of the CCP from infiltrating our data and our telecommunications network.

Madam Speaker, I urge all of my colleagues to support this bill, and I reserve the balance of my time.

Mr. PALLONE. Madam Speaker, I have no additional speakers, and I reserve the balance of my time.

Mr. SCALISE. Madam Speaker, I yield 2 minutes to the gentleman from Ohio (Mr. LATTA), the ranking member of the Communications and Technology Subcommittee.

Mr. LATTA. Madam Speaker, I thank the gentleman from Louisiana, my good friend, the whip of the Republican Party here in the House, for yielding.

Madam Speaker, I rise today in support of H.R. 3919, the Secure Equipment Act of 2021, which was introduced by Representatives Scalise and Eshoo.

This bill takes an important step to strengthen the security of our communications network from bad actors like Huawei. The Communist Chinese Party and its allies have been working for years to find ways to access American networks and enter our markets. Our national security agencies agree that Huawei and other untrusted vendors pose an unacceptable risk to our national security. Today, we are sending another strong signal that America will hold China accountable.

Last Congress, we passed the Secure and Trusted Communications Act into law, which took a great first step to secure our networks by prohibiting Federal funds to be used to purchase untrusted equipment and services, still allowing untrusted vendors to enter our market if purchased by private dollars.

H.R. 3919 would strengthen our national security and close this loophole by prohibiting the FCC from licensing any communication equipment by an entity on the Commission’s covered list, regardless of whether it was bought using public dollars.

It is critical that we work to stay one step ahead of our adversaries, and this bill would advance our security as 5G is deployed across the country.

Madam Speaker, I urge my colleagues to support this measure.

Mr. PALLONE. Madam Speaker, I reserve the balance of my time.

Mr. SCALISE. Madam Speaker, I yield 1 minute to the gentleman from

Indiana (Mr. PENCE), my friend and also a member of the committee.

Mr. PENCE. Madam Speaker, I thank the gentleman from Louisiana for yielding.

Madam Speaker, I rise today in staunch support of the bipartisan Secure Equipment Act of 2021.

Hoosiers back home in my home State of Indiana rely heavily on telecom companies to connect them with the critical services they need, particularly healthcare through telehealth. When foreign adversaries, like Communist China, try to prey upon these companies, they are in turn attempting to prey upon hardworking Americans like my constituents. That is why I am proud today to join my colleagues in supporting this vital legislation that would ensure the Federal Government prevents any further Chinese state-backed equipment from being used here in the United States.

This bill is vital to our national security, and I urge my colleagues on both sides of the aisle to support it.

Mr. PALLONE. Madam Speaker, does the whip have any additional speakers?

Mr. SCALISE. Madam Speaker, the gentleman does not, and I am prepared to close.

Mr. PALLONE. Madam Speaker, I reserve the balance of my time.

Mr. SCALISE. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I would just again join, along with my colleague, ANNA ESHOO from California, in urging all Members of the House to pass the Secure Equipment Act and protect the privacy of data from Americans as well as that sensitive information that flows across networks that is also held by the government.

Let's delist and not certify companies that have already been deemed by the FCC to be national security threats. I urge all of my colleagues to support this bill, and I yield back the balance of my time.

Mr. PALLONE. Madam Speaker, I would urge, again, bipartisan support. This is an important next step in our effort to try to secure our equipment and prevent foreign actors, such as the Chinese, from interfering with our national security, and I yield back the balance of my time.

Ms. ESHOO. Madam Speaker, I rise in strong support of H.R. 3919, the Secure Equipment Act of 2021, as amended.

For over a decade, I have raised concerns about how the vulnerabilities in our telecommunications infrastructure directly impact our national security. On November 2, 2010, I wrote to the Chairman of the Federal Communications Commission (FCC) expressing grave concerns about Huawei and ZTE, which have opaque relationships with the Chinese government.

Sadly, in the intervening eleven years, telecommunications companies have invested hundreds of millions of dollars in equipment made by Huawei and ZTE because the equipment is the cheapest available.

On March 12, 2020, Congress passed and the President signed into law the Secure and

Trusted Communications Networks Act of 2019 (STCNA), which directed the FCC to: (i) establish a list of companies deemed to be a national security threat; (ii) prohibit the use of federal funds for purchasing equipment made by those companies; and (iii) authorize funding for U.S. carriers to rip and replace equipment made by those companies. The FCC's list includes Huawei, ZTE, and other companies linked to the Chinese government.

STCNA was a significant step forward for our national security. However, U.S. companies can still privately purchase equipment from these companies. This allows potentially vulnerable equipment into our wireless systems which is a threat to our national security because compromised equipment can include hard-to-detect surveillance capabilities.

On June 15, 2021, Representative STEVE SCALISE and I introduced H.R. 3919 to prohibit the FCC from approving any telecommunications equipment made by companies deemed to be a national security threat. Senators MARCO RUBIO and ED MARKEY have companion legislation in the Senate. The legislation is supported by the FCC's Democratic Acting Chairwoman Jessica Rosenworcel and Republican Commissioner Brendan Carr.

The bill was considered and favorably advanced by voice vote, first by the House Subcommittee on Communications and Technology and then by the Committee on Energy and Commerce. The companion bill was favorably advanced by the Senate Committee on Commerce, Science, and Transportation.

As I stated when STCNA was being considered by our chamber, no one bill can fully protect our telecommunications networks. The threats we face are constantly evolving, and Congress must remain diligent in ensuring our communications are secure, private, and reliable.

H.R. 3919 is a highly important and necessary complement to STCNA and I urge my colleagues to vote for it.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New Jersey (Mr. PALLONE) that the House suspend the rules and pass the bill, H.R. 3919, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. GOOD of Virginia. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

OPEN RAN OUTREACH ACT

Mr. PALLONE. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4032) to provide outreach and technical assistance to small providers regarding the benefits of Open RAN networks, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4032

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Open RAN Outreach Act".

SEC. 2. OUTREACH AND TECHNICAL ASSISTANCE TO SMALL PROVIDERS REGARDING OPEN RAN NETWORKS.

(a) *IN GENERAL.*—The Assistant Secretary shall conduct outreach and provide technical assistance to small communications network providers—

(1) *to raise awareness regarding the uses, benefits, and challenges of Open RAN networks and other open network architectures; and*

(2) *regarding participation in the Wireless Supply Chain Innovation Grant Program established under section 9202(a)(1) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283).*

(b) *DEFINITIONS.*—In this section:

(1) *ASSISTANT SECRETARY.*—The term "Assistant Secretary" means the Assistant Secretary of Commerce for Communications and Information, acting through the head of the Office of Internet Connectivity and Growth.

(2) *OPEN NETWORK ARCHITECTURE.*—The term "open network architecture" means Open RAN networks and other network elements that follow a set of published open standards for multi-vendor network equipment interoperability, including open core and open transport.

(3) *OPEN RAN NETWORK.*—The term "Open RAN network" means a wireless network that follows the Open Radio Access Network approach to standardization adopted by the O-RAN Alliance, Telecom Infra Project, or Third Generation Partnership Project (3GPP), or any similar set of published open standards for multi-vendor network equipment interoperability.

Amend the title so as to read: "A bill to provide outreach and technical assistance to small providers regarding Open RAN networks, and for other purposes."

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New Jersey (Mr. PALLONE) and the gentleman from Ohio (Mr. LATTA) each will control 20 minutes.

The Chair recognizes the gentleman from New Jersey.

GENERAL LEAVE

Mr. PALLONE. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 4032.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from New Jersey?

There was no objection.

Mr. PALLONE. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise in strong support of H.R. 4032, the Open RAN Outreach Act.

Open RAN, or Open Radio Access Network, technology is an emerging wireless network architecture that has the potential to drive 5G innovation forward. But like any new technology, we still have much to learn about the possibilities, complexities, and challenges of Open RAN. This is especially true for smaller communications providers.

This bill steps up to the challenge by providing small communications providers with the support they need to